DRAFT CSSG RECOMMENDATION

DOE G 423.X

IV.12 Violation of a TSR.
d.

“To qualify as a TSR violation the failure to meet the intent of the referenced program would need to be significant enough to render the DSA summary invalid".

Add the following paragraph: For example, a typical fissile mass limit violation, as the example on p. 64 provides, would not render the DSA summary invalid due to the significant number of barriers that would still exist and that would have to be violated to reach the critical state. This why fissile mass limits have not been judged to be TSR level controls and why they are usually categorized according to DOE Orders as abnormal events or even non-reportable. Thus making fissile mass limits LCOs would make their violation a much more significant event (a TSR violation) than would be consistent with the Occurrence Reporting Order and related regulations.

Delete section IV.14

Replace section IV.10 e. with the following

e. Fire Protection, HVAC, Natural Phenomena Hazards (NPH) and Criticality Controls

Fire poses the most significant risk in some DOE facilities. For those facilities, certain key fire protection LCOs will need to be developed as dictated by the DSA accident analysis and the Fire Hazards Analysis (FHA) required by DOE O 420.1. The TSR document may need to include a reference to general safety controls provided by the fire protection program but it also needs to identify specific controls (usually LCOs) for any fire protection equipment that has been identified in the DSA as performing a safety function. Similarly, the HVAC systems and their filters may require TSRs for those elements of the system that have been identified with a safety function in the DSA. The NPH assessment required by DOE O 420.1 may also result in controls (mainly related to NPH detection and warning devices) that should be incorporated into the TSR document.

Criticality controls must be developed to ensure that operations remain subcritical under all normal and credible abnormal conditions. Criticality controls may derive directly from the DSA or supporting CSEs. However, these are typically developed and documented in a criticality safety evaluation (CSE) that supports the DSA. Some of these may be appropriate for inclusion as explicit TSRs or to have TSR level surveillance requirements. TSR level controls should be identified on a case by case basis and graded according to the guidance in DOE-STD-3009-00, Change Notice No. 1 with regard to classification of controls.

DRAFT CSSG RECOMMENDATION

Generally speaking, only those criticality controls involving passive or active engineered features warrant consideration for elevation to the level of an explicit TSR. Even here the significant defense in depth usually implemented for fissile operations and documented in a CSE frequently results in these engineered controls representing only a modest fraction of the total defense in depth. Said differently, the loss of any one of these engineered controls would not generally result in a singly contingent condition and thus many engineered features would not warrant TSR level status. Important active engineered features should be covered under TSRs and LCOs, while passive design features should be captured in the authorization bases as design features credited for safety. In determining the frequencies for surveillance, the likely failure modes and time frames of the specific SSCs should be considered. Conversely, the benefits of functionally classifying procedural administrative criticality controls and subsequently capturing them explicitly in TSRs are minimal, provided these controls impose double contingency. Thus, procedural administrative controls should not be explicitly captured in TSRs. Excessive use of procedural controls for the primary purpose of minimizing the number of explicit criticality safety related TSRs is not acceptable.